

Entender o perfil de regras do Snort 3 e o perfil de CPU na GUI do FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Visão geral do recurso](#)

[Criação de perfil](#)

[Criador de Perfil da Regra](#)

[Criação de perfil de regra de operação](#)

[Menu de criação de perfil do Snort 3](#)

[Iniciar criação de perfil de regra](#)

[Resultados do criador de perfil da regra](#)

[Faça o download dos resultados](#)

[Criação de perfil da CPU](#)

[Visão geral do Snort 3 CPU Profiler](#)

[Guia CPU Profiling](#)

[Explicação dos resultados do CPU Profiler](#)

[Resultado do CPU Profiler - Baixar Instantâneo](#)

[Filtragem de resultado da criação de perfil da CPU](#)

Introdução

Este documento descreve a regra Snort 3 e o recurso de criação de perfil de CPU adicionados ao FMC 7.6.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Snort 3
- FMC (Secure Firepower Management Center, Centro de gerenciamento seguro do Firepower)
- Defesa contra ameaças (FTD) Secure Firepower

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Este documento se aplica a todas as plataformas Firepower
- Secure Firewall Threat Defense Virtual (FTD) executando a versão de software 7.6.0
- Secure Firewall Management Center Virtual (FMC) executando a versão de software 7.6.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral do recurso

- A criação de perfis de regra e CPU já existia no Snort, mas era acessível apenas por meio da CLI do FTD. O objetivo desse recurso é estender os recursos de criação de perfil e torná-lo mais simples.
- Ative o debug intrusion rule performance issues (depurar problemas de desempenho de regras de intrusão) e ajuste as configurações das regras por conta própria antes de entrar em contato com o TAC para obter ajuda na solução de problemas.
- Entenda quais módulos têm desempenho insatisfatório quando o Snort 3 está consumindo muita CPU.
- Crie uma maneira fácil de depurar e ajustar as políticas de Intrusão e Análise de rede para obter melhor desempenho.

Criação de perfil

- O Rule Profiling e o CPU Profiling são executados no FTD e seus resultados são armazenados no dispositivo e extraídos pelo FMC.
- Você pode executar várias sessões de criação de perfil simultaneamente em dispositivos diferentes.
- Você pode executar o Rules Profiling e o CPU Profiling ao mesmo tempo.
- Em caso de alta disponibilidade, a criação de perfil só pode ser iniciada no dispositivo que está ativo no início da sessão.
Para configurações em cluster, a criação de perfis pode ser executada em cada nó no cluster.
- Se uma implantação for acionada enquanto houver uma sessão de criação de perfil em andamento, um aviso será exibido ao usuário.

Se o usuário optar por ignorar a advertência e a disponibilização, isso cancelará a sessão de criação de perfil atual e o resultado do profiler mostrará uma mensagem relacionada a isso.

Uma nova sessão de criação de perfil precisa ser iniciada sem ser interrompida por uma implantação para obter os resultados reais da criação de perfil.

Criador de Perfil da Regra

- O criador de perfil de regra do Snort 3 coleta dados sobre a quantidade de tempo gasto no

processamento de um conjunto de regras de intrusão do Snort 3, destacando assim possíveis problemas, mostrando regras com desempenho insatisfatório.

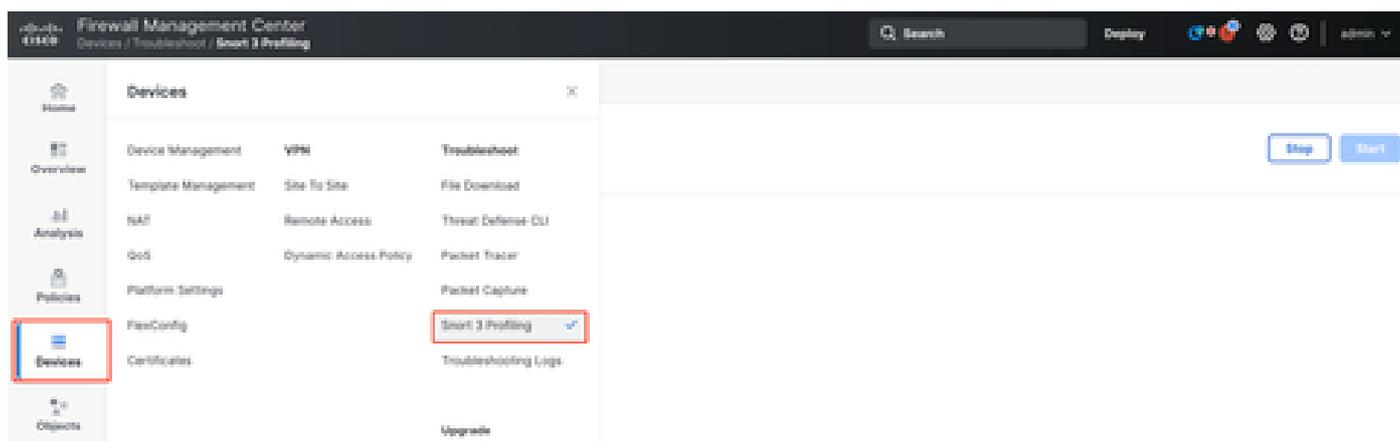
- O Rule Profiler exibe as regras de 100 IPS que levaram mais tempo para serem verificadas.
- Disparar o Rule Profiler não requer recarregamento ou reinicialização do Snort 3.
- Os resultados da criação de perfil da regra são salvos no formato JSON no diretório `/ngfw/var/sf/sync/snort_profiling/` e sincronizados no FMC.
- O Rule Profiler está dentro do Snort 3 e inspeciona o tráfego com o mecanismo de detecção de intrusão Snort 3; ativar a criação de perfil de regra não tem nenhum impacto notável no desempenho.

Criação de perfil de regra de operação

- O tráfego deve estar fluindo pelo dispositivo
- Iniciar criação de perfil de regra selecionando um dispositivo e clicando no botão Iniciar
 - Iniciar uma sessão de criação de perfil cria uma tarefa que pode ser monitorada em Notificações, em Tarefas
- A duração padrão de uma sessão de criação de perfil da regra é de 120 minutos
 - A sessão de criação de perfil de regra pode ser interrompida mais cedo, antes da conclusão, pressionando o botão Parar
- Os resultados podem ser visualizados na GUI e baixados
- O Histórico de criação de perfil exibe os resultados das sessões de criação de perfil anteriores. O usuário pode inspecionar um resultado de criação de perfil específico clicando em uma placa no painel do lado esquerdo do Histórico de criação de perfil.

Menu de criação de perfil do Snort 3

A página Profiling (Criação de perfil) pode ser acessada no menu Devices > Snort 3 Profiling. A página contém a criação de perfil de Regra e CPU, divididas em duas guias.



Dispositivos

Iniciar criação de perfil de regra

Para iniciar uma sessão de criação de perfil de regra, clique em Iniciar. A sessão é automaticamente interrompida após 120 minutos.

Um usuário não pode configurar a duração da sessão de criação de perfil, mas pode interrompê-la antes que decorram as duas horas.

Rule Profiling CPU Profiling

Select device for Rule Profiling

FTD1

Stop Start

Rule Profiling Results - FTD1 - 22 minutes ago

Start: 2025-01-16 10:35:40 IST Access Control Policy: test VDB: 392 Snort Version: 3.1791-121
Finish: 2025-01-16 10:37:10 IST Access Control Policy revision time: 2025-01-15 13:15:26 IST LSP: lsp-rel-20250114-1341 Device Version: 7.6.0-113

Criação de perfil de regra

Rule Profiling CPU Profiling

Select device for Rule Profiling

FTD1

Running

Stop Start



Rule Profiling started 8 seconds ago

Profiling takes around 120 minutes. The task manager will send notification when the profiling task is complete.

Executando

Depois que a sessão de criação de perfil da regra for iniciada, uma tarefa será criada. Isso pode ser verificado em Notificações > Tarefas.

Deployments Upgrades Health Tasks Show Pop-up Notifications

20+ total 0 waiting 3 running 0 retrying 20+ success

1 failure

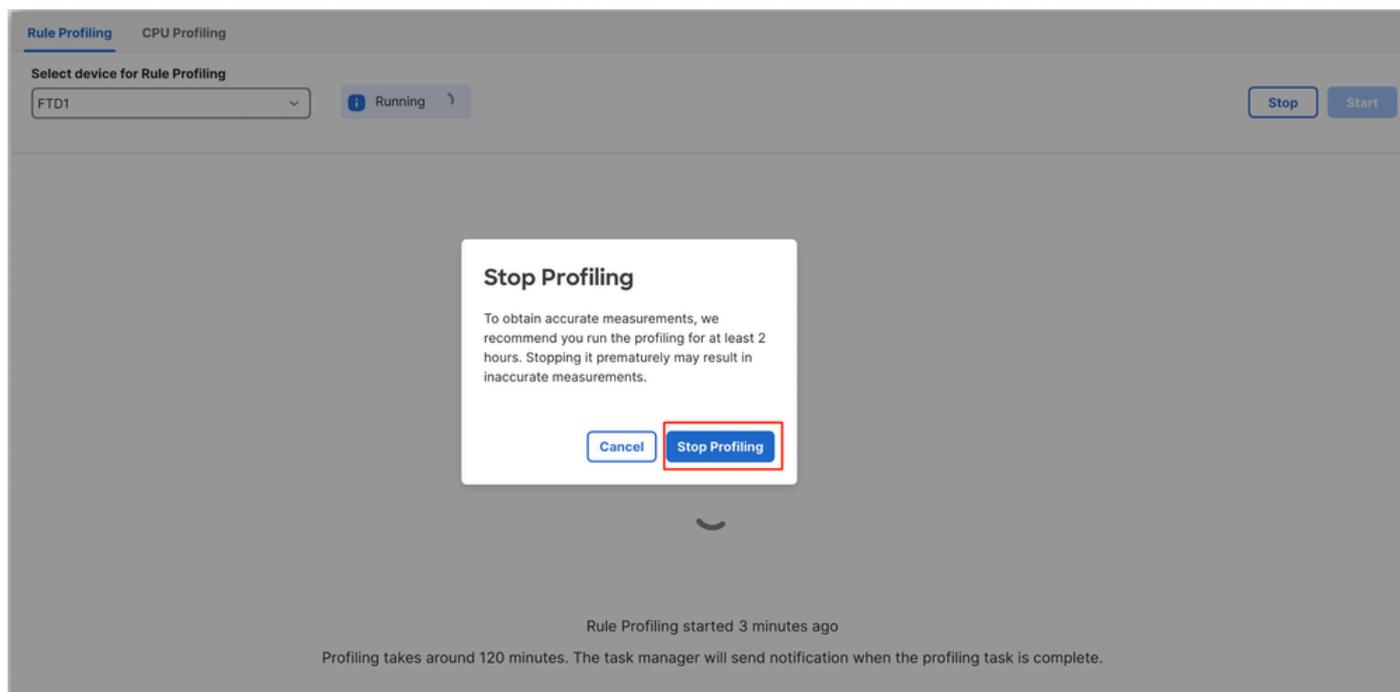
Filter

Rule profiler

Generate Rule Profiling File 2m 6s
Generate rule profiling file for FTD1
Remote status: Generating rule profiling file

Tarefas

Para interromper uma sessão de criação de perfil de regra que esteja em andamento, caso você precise interrompê-la antes da interrupção automática, clique em Parar e confirme.



Parar criação de perfil

Depois de selecionar um dispositivo, o resultado mais recente da criação de perfil é automaticamente exibido na seção Resultados da criação de perfil da regra.

A tabela contém estatísticas das regras que levaram mais tempo para serem processadas classificadas em ordem decrescente pelo tempo total (em microssegundos (μ s)) que elas levaram.consumido.

Git:Sid	Rule Description	% of Snort Time	Rev	Checks	Matches	Alerts	Time (μ s)	Avg/Check	Avg/Match	Avg/Non-Match	Timeouts	Suspends
1:23224	EXPLOIT-KIT Redkit exploit kit landing page Requested - 8Digit.html	0.00033%	13	17	0	0	143	8	0	8	0	0
1:28585	FILE-PDF Adobe Acrobat Reader OTF font head table size overflow atte...	0.00001%	8	16	0	0	49	3	0	3	0	0
1:47030	MALWARE-CNC Win.Malware.Innaput variant outbound connection	0.00001%	1	37	0	0	44	1	0	1	0	0
1:37651	MALWARE-TOOLS Win.Trojan.Downloader outbound connection attempt	0.00001%	3	6	0	0	42	7	0	7	0	0

Resultados

Resultados do criador de perfil da regra

A saída do criador de perfil de regra para uma regra de IPS inclui estes campos:

- % de tempo de Snort - Tempo gasto no processamento da regra, relativo ao tempo da operação do Snort 3
- Verificações - Número de vezes que a regra de IPS foi executada
- Correspondências - Número de vezes que a regra de IPS foi totalmente correspondida
- Alertas - número de vezes que a regra IPS disparou um alerta IPS
- Tempo (μ s) - Tempo em microssegundos Gasto pelo Snort na verificação da regra de IPS
- Média/Verificação - Tempo médio que o Snort passou em uma verificação da regra
- Média/Correspondência - Tempo médio que o Snort passou em uma verificação que

resultou em uma correspondência

- Média/Sem Correspondência - Tempo médio que o Snort passou em uma verificação que não resultou em uma correspondência
- Intervalos - Número de vezes em que a regra excedeu o Limite - Tratamento de Regras configurado nas Configurações de Desempenho Baseadas em Latência da política de CA
- Suspende - Número de vezes que a regra foi suspensa devido a algumas violações de limite consecutivas

Faça o download dos resultados

- O usuário pode baixar o resultado da criação de perfil ("instantâneo") clicando no botão "Download Snapshot". O arquivo baixado está no formato .csv e contém todos os campos da página de resultados da criação de perfil.
- Extraia do arquivo .csv do instantâneo:

Device,Start Time,End Time,GID:SID,Rule Description,% of Snort Time,Rev,Checks,Matches,Alerts,Time (µs) Avg/Check Avg/Match Avg/Non-Match Timeouts Suspends

Exibição instantânea de arquivo .csv:

Rule_Profiling_172.16.0.102_2024-03-13 11_08_41

Device	Start Time	End Time	GID:SID	Rule Description	% of Snort Time	Rev	Checks	Matches	Alerts	Time (µs)	Avg/Check	Avg/Match	Avg/Non-Match	Timeouts	Suspends
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	2000:1000001	TEST 1	0.00014	1	4	4	1	284	71	71	0	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:28595	FILE-PDF Adobe Acrobat Reader OTF font head table size overflow attempt	0.00006	8	4	0	0	113	28	0	28	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:23224	EXPLOIT-KIT Redkit exploit kit landing page Requested - 8DigiL.html	0.00003	13	4	0	0	64	16	0	16	0	0
172.16.0.102	2024-03-13 11:05:41	2024-03-13 11:07:21	1:55993	PROTOCOL-ICMP Microsoft Windows IPv6 DNSL option record denial of service attempt	0.00002	1	4	0	0	32	8	0	8	0	0

Instantâneo

Criação de perfil da CPU

Visão geral do Snort 3 CPU Profiler

- O criador de perfil de CPU define o tempo de CPU gasto pelos módulos/inspetores do Snort 3 para processar pacotes em um determinado intervalo de tempo. Ele dá uma ideia de quanto CPU cada módulo está consumindo, em relação ao total de CPU consumido pelo processo Snort 3.
- O uso do CPU Profiler não requer a recarga da configuração nem a reinicialização do Snort 3, evitando, assim, períodos de inatividade.
- O resultado do CPU Profiler exibe o tempo de processamento gasto por todos os módulos durante a última sessão de criação de perfil.
- Os resultados da criação de perfil da CPU são salvos no formato JSON no diretório `/ngfw/var/sf/sync/cpu_profiling/` e sincronizados no diretório `/var/sf/peers/<device UUID>/sync/cpu_profiling` do FMC.
- Uma nova página de criação de perfil do Snort 3 foi adicionada na interface do usuário do FMC

- Esta página pode ser acessada a partir da guia Dispositivos > Perfil do Snort 3 > Perfil da CPU
- Use Download Snapshot na guia Criação de perfil da CPU para fazer o download de um instantâneo dos resultados da criação de perfil no formato CSV.

Guia CPU Profiling

A página Perfil da CPU é acessada a partir da guia Dispositivos > Perfil do Snort 3 > Perfil da CPU.

Ele contém um seletor de dispositivos, os botões Iniciar/Parar, o botão Fazer download do instantâneo, uma seção de resultados de criação de perfil e uma seção Histórico de criação de perfil no lado esquerdo que é expandida ao clicar nele.

Criação De Perfil Da Cpu

Para iniciar uma sessão de criação de perfil da CPU, clique em Iniciar. Esta página é mostrada quando a sessão é iniciada.

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
daq	100	6674110782	893694	100
perf_monitor	0	39946	5	0
firewall	0	16360	2	0
mpse	0	2181	0	0

Iniciar

State Profiling CPU Profiling

Select device for CPU Profiling: FTD1 Running

Dismiss all notifications

CPU profiler
Generate CPU Profiling File
Generate CPU profiling file for FTD1
Remote status: Generating CPU profiling file

CPU Profiling started 8 seconds ago
Profiling takes around 120 minutes. The task manager will send notification when the profiling task is complete.

Executando

Depois que a sessão de criação de perfil da CPU for iniciada, uma tarefa será criada. Isso pode ser verificado em Notificações > Tarefas.

! Deployments Upgrades ! Health ! **Tasks** [Download] [Toggle]

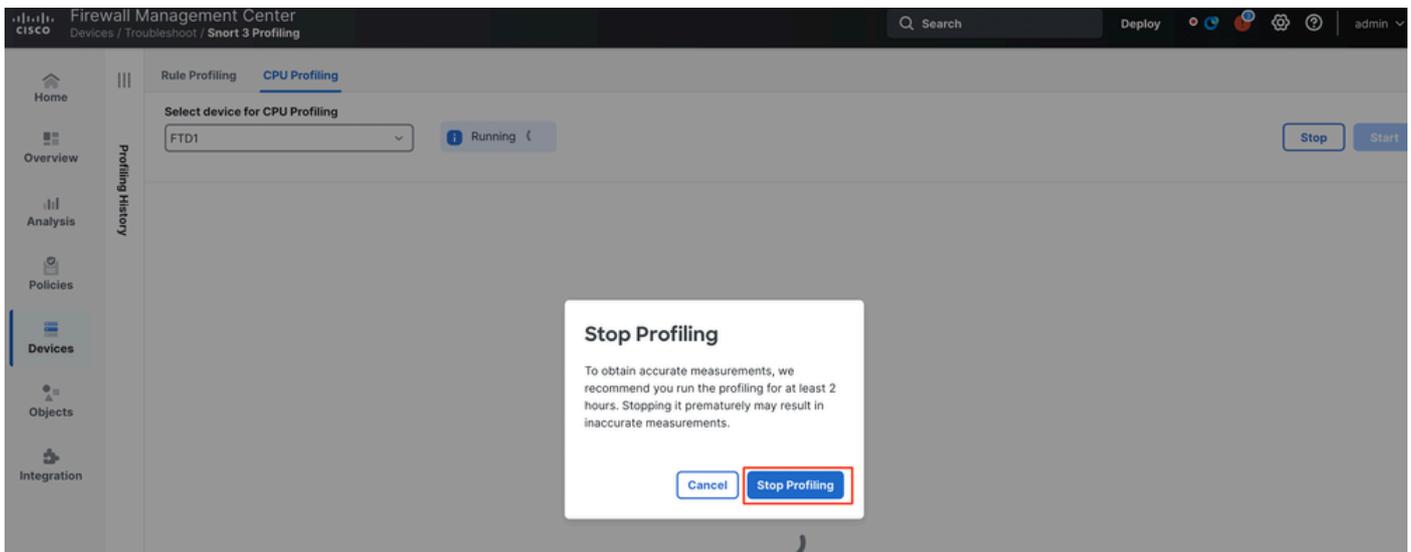
20+ total | 0 waiting 2 running 0 retrying 20+ success
1 failure

 CPU profiler

Generate CPU Profiling File
Generate CPU profiling file for FTD1
Remote status: Generating CPU profiling file

Tarefas

- Para parar uma sessão de criação de perfil de CPU em andamento, clique em Parar.
- Uma caixa de diálogo de confirmação é exibida. clique em Stop Profiling.



Parar Execução

O resultado mais recente da criação de perfil é exibido na seção Resultados da criação de perfil da CPU.

CPU Profiling Results - FTD1 (29 seconds ago) [Download Snapshot](#)

Start: 2025-01-16 11:20:00 EST Access Control Policy: local VM: 363 Snort Version: 3.9.8.1-101
 Ends: 2025-01-16 11:23:24 EST Access Control Policy violation time: 2025-01-16 13:15:24 EST LBP: log-net-20250116-10341 Device Version: 18.0-110

Filter by % of Short time Total 4

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
diag	100	386446899	900380	100
perf_monitor	0	1662	4	0
firewall	0	933	3	0
mpise	0	101	0	0

Resultados

Explicação dos resultados do CPU Profiler

- A coluna "Módulo" indica o nome do módulo/inspetor.
- A coluna "% de Tempo Total de CPU" indica o percentual de tempo gasto pelo módulo em relação ao tempo total gasto pelo Snort 3 no tráfego de processamento. Se esse valor for consideravelmente maior do que o de outros módulos, o módulo estará contribuindo mais para o desempenho insatisfatório do Snort 3.
- "Tempo (µs)" representa o tempo total, em microssegundos, de cada módulo.
- "Média/Verificação" representa o tempo médio gasto pelo módulo para cada vez que ele é chamado.
- "% Caller" indica o tempo gasto pelo submódulo (se configurado) em relação ao módulo principal. Ele é usado principalmente para fins de depuração de desenvolvedor.

Resultado do CPU Profiler - Baixar Instantâneo

- O usuário pode baixar o instantâneo do resultado da criação de perfil clicando em Download Snapshot. O arquivo baixado está no formato .csv e contém todos os campos da página de

resultados da criação de perfil, como mostrado neste exemplo.

- Extraia do arquivo .csv do instantâneo:

CPU_Profiling_FTD1_2025-01-16 00_55_45

Device	Start Time	End Time	Module	% Total of CPU time	Time (µs)	Avg/Check	%/Caller
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	daq	100	366446909	900360	100
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	perf_monitor	0	1662	4	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	firewall	0	923	2	0
FTD1	2025-01-16 00:50:30	2025-01-16 00:53:34	mpse	0	101	0	0

Instantâneo

Filtragem de resultado da criação de perfil da CPU

Os resultados da criação de perfil podem ser filtrados usando:

- "Filtrar por % do tempo de Snort" - permite filtrar módulos cuja execução levou mais de n% do tempo de criação de perfil.
- Pesquisa - permite que você faça uma pesquisa de texto em qualquer campo presente na tabela de resultados.

Qualquer coluna, exceto "Módulo", pode ser classificada clicando em seu cabeçalho.



Filter by % of Snort time 0.20 % Total 10

Module	% Total of CPU time	Time (µs)	Avg/Check	% Caller
rule_eval	20.89	26138283	3	20.89
mpse	14.11	17661177	0	14.11

Resultados

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.